CIO*Update*

July 14, 2000

Cyber Security

United States Department of Energy CIO Update 5

Message from the CIO

Defending DOE's Cyberspace

John Gilligan
CIO, Department of Energy

Over the past year, the Department has received a great deal of negative attention regarding reported weaknesses in protecting sensitive information and related systems and networks. As CIO, I find the headlines painful and, at times, embarrassing. These news stories have left the public with the impression that DOE is doing a poor job of protecting the systems and information for which it is responsible. This issue of CIO Update focuses on some common cyber security weaknesses as well as a number of security initiatives within the Department and across the Federal government.

Perhaps it is useful to share my personal perspective on how DOE's cyber security stacks up against that of other agencies. Having worked in the Department of Defense and having served as co-chair of the Federal CIO Council's Security Subcommittee, I have a reasonably good perspective on the state of security across the Federal government. In general, the state of security protection within DOE is comparable with most agencies and most private organizations. This assessment, however, does not mean that we can relax.

The need to protect unclassified systems and information has grown dramatically over the past few years in response to the increasing threat caused by rapid advances in the Internet and internetworking technologies. This increased threat warrants significant upgrades to our protection to avoid business disruptions and loss or compromise of valuable systems or data. DOE sites are now planning and implementing these upgrades, but it is a significant change and not a quick process. Protection of our classified systems is modeled after Department of Defense policy and practices, and in many cases it has proved adequate. However, for highly sensitive nuclear weapons information, recent studies have made it clear that DOE needs to implement much tighter protection measures, in most cases paralleling the protection afforded the Nation's most sensitive intelligence-related information. The Department is developing an initiative to provide major upgrades to classified systems security at our nuclear weapons facilities.

Many of the most common cyber security vulnerabilities cannot be rationalized as the result of a lack of resources or the absence of proven solution approaches. Common vulnerabilities include easily guessed passwords (especially using automated tools) or no password controls; systems not patched to fix known hacker pathways; and "back door" Internet connections that become avenues of attack for an entire site. These are management, not technical, challenges. I have found that the single biggest cyber security challenge facing the Department is the failure of line management to treat our computers and the information that they manage as strategic corporate resources that require aggressive management. In short, we need to proactively manage our computers as a prerequisite to providing good security.

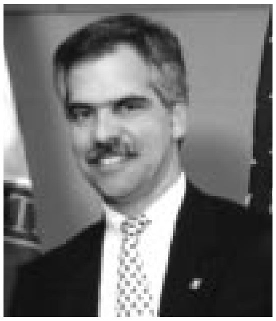
A second major challenge facing managers, in particular for unclassified systems, is determining how much protection is enough. Adequate protection for classified systems is usually prescribed by regulation, but unclassified systems rely on an assessment of risk and consequence of security incidents to govern the security approach. Site management must make a positive decision about what is adequate. This is a very difficult task requiring continued dialogue between security professionals and line management.

continued to page 3

In This Issue

Questions? Contact Howard Landon. Telephone: 202-586-6344; email: howard.landon@hq.doe.gov

OA Reviews Effectiveness



Mr. Glenn Podonsky, Director of the Office of Independent Oversight and Performance Assurance.

The Office of Independent Oversight and Performance Assurance (OA), directed by Mr. Glenn Podonsky, provides an independent review of the effectiveness of safeguards and security, emergency management, and cyber security policies and programs throughout the DOE complex. OA was established by the Secretary of Energy in May 1999. OA reports directly to the Secretary. Since summer 1999, OA has conducted 15 reviews including comprehensive inspections, follow-up reviews, and external network security assessments.

OA has an extensive remote cyber security laboratory dedicated to testing cyber security features from the Internet, including unannounced inspections and penetration testing. OA employs a variety of techniques to assess a site’s cyber security features, including penetration testing, firewall rules reviews, intrusion detection evaluation, and modem testing. These tests are conducted by experts who are thoroughly familiar with the latest hacker techniques and methods. During a comprehensive inspection, OA conducts internal performance testing on both classified and unclassified networks. OA combines extensive performance testing with a programmatic review of key elements that include leadership, responsibilities and authorities, risk management and planning, policy, guidance, procedures, technical implementation, feedback, and improvement.

Where vulnerabilities are identified by OA, OCIO works with site and line management organizations to achieve rapid resolution. Recommendations for improvements made by OA’s reviews are enforced via mandated corrective action plans. These plans are tracked by the DOE Security Council, which is chaired by the DOE Security Czar, General Eugene Habiger. OA performs follow-up reviews to find clear evidence that sites are making progress. One positive trend noted by OA is that many sites have established their own programs for performing regular scans of networks and tests of security features. More information is available on the OA web site (http://tis.eh.doe.gov/iopa/).

HQ Review Reveals Weaknesses

In April 2000, the DOE Office of Independent Oversight and Performance Assurance (OA) reviewed Headquarters (HQ) unclassified cyber security program, including a programmatic review and testing of controls to prevent or limit access to the HQ information network. The review found significant deficiencies. The problems centered on fragmented management systems and practices as well as the interconnection of all HQ networks, which allows an office with weak security to undermine the effectiveness of better-managed offices.

Weaknesses included: a lack of HQ-wide procedures on configuration management; absence of consistent policy on external connections, modems, and foreign national access; lack of minimum cyber security requirements for each local area network in HQ; and lack of a formal process to evaluate performance, identify cyber security vulnerabilities, and correct them. HQ risk assessments have not been rigorous enough and have not considered the shared risk of the interconnected network. OCIO attempts to address these problems have been hampered by a lack of real and perceived authority.

OA recommended immediate and long-term actions and will follow-up to measure progress. Immediate actions include designating OCIO as the single focus point for HQ Cyber Security and establishing HQ-wide processes and procedures. Longer-term actions include adopting best practices and a more proactive risk assessment program. On June 8, 2000, the Deputy Secretary directed OCIO to serve as HQ's central cyber security authority. HQ will be managed as a single entity with a consistent, site-wide cyber security approach. CIO Operations is responsible for HQ cyber security policies, processes, and procedures, which will be coordinated through a HQ Cyber Security Working Group with a representative from each HQ office. OCIO is addressing HQ's problems via network connection policies, an integrated security configuration management process, and a security self-assessment process.

OCIO will provide the Secretary with regular updates on HQ’s progress. Moreover, the Department believes that HQ must set the standard for the rest of the Department on how to implement security of cyber systems. The Secretary and the CIO are fully committed to ensuring that HQ is a model for the rest of the Department.

Focus on Departmental Cyber Security

Since the spring of 1999, the Secretary of Energy and OCIO have emphasized a Departmentwide focus on cyber security. Initially, the effort focused on the Defense laboratories and production facilities, implementing aggressive programs to upgrade and verify fixes at these facilities last summer and fall. This focus has been extended to all DOE sites, and the Department has completely restructured its cyber security program.

The restructured program emphasizes an increased awareness of cyber security, backed by mechanisms and policy. A Departmentwide Cyber Security Office has been created under OCIO. The Department requires work "stand downs" at all sites to conduct security awareness training. Four new policies and two new guidelines have been issued. Metrics are employed to evaluate progress at each site. CIAC has been doubled in size and its role has been increased. Each DOE site is required to develop a detailed, site-specific cyber security program plan, describing the implementation of cyber security protection. A Departmentwide cyber security training program has been deployed to improve the skills of system administrators. There is a separate training course for line managers. Each site has significantly upgraded its protection via firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerability.

Message from the CIO continued from page 1

The bottom line is that over the past 12 months the Department has made enormous progress in improving its cyber security posture. Great credit must be given to the many individuals at each site who have worked this issue aggressively. However, we are not at the end of this journey. We are in the middle of the effort. Continued focus on the initiatives described in this issue, as well as individual site programs, are needed to ensure that the Department stays out of the spotlight and is confident of ensuring adequate security protection for important assets. I am confident that we will reach this state during the next 12-18 months.

John M. Gilligan
Chief Information Officer, Department of Energy
202-586-0166   E-mail: cio@hq.doe.gov

Top 10 Internet Security Threats

A few software vulnerabilities account for the majority of successful cyber attacks. System administrators might not correct these flaws because they simply do not know which of over 500 potential problems are the most dangerous and they are too busy to fix all of them. In response to a Presidential initiative to deal with cyber attacks, a team of national computer security and software experts authored The Ten Most Critical Internet Security Threats (http://cio.gov/docs/whatsnew.htm), providing a consensus list to help system administrators.

The Top 10 Internet Security Threats

1: *The Berkeley Internet Name Domain (BIND)* package allows Internet sites to be located by name, but its weaknesses make it a favorite target for attacks that erase system logs or install tools to gain administrative access.
2: *Vulnerable Common Gateway Interface (CGI)* programs are easy for attackers to locate, and they operate with the privileges of the web server software.
3: Multiple vulnerabilities in Remote Procedure Calls (RPCs) are being actively exploited and are the main cause of the recent rash of denial of service attacks.
4: *Flaws in Microsoft's Internet Information Server (IIS)* are being used by malicious intruders to run remote commands with administrator privileges.
5: *Sendmail,* the program that sends, receives, and forwards most e-mail on UNIX and Linux systems, has flaws that allow hackers to trick the program into sending its password file to the hacker's machine.
6: *UNIX and Linux systems* are vulnerable to intruders via "sadmind" and "mountd" services.
7: Improperly configured global *file sharing services* can expose critical system files or give full file system access to any hostile party connected to the network.
8: *User IDs* at the root/administrator level may have easily-guessed or widely-known default passwords that busy administrators may neglect to change, giving attackers an easy way into the system.
9: The popular remote access mail protocols, *IMAP and POP,* allow users to access their e-mail from internal and external networks. They are especially vulnerable because openings are frequently left in firewalls to allow for external e-mail.
10: *The Simple Network Management Protocol (SNMP)* uses an unencrypted "community string" as its authentication mechanism, and attackers exploit this weakness to reconfigure or shut down devices remotely.

CSA and CSPP Status

DOE’s Cyber Security Architecture (CSA) Version 2.3, dated May 30, 2000, is now in the Directives process for review and comment. The CSA provides a Departmen-wide framework for a common understanding of the design, implementation, and operation of DOE cyber security resources and systems. It covers unclassified data networks, host systems, and applications. For more information, contact Stanley P. Wujcik, Cyber Security team lead for the CSA, (Telephone: 301-903-3434 or email: stanley.wujcik@hq.doe.gov).

Cyber Security Program Plans (CSPPs) are being reviewed by the Cyber Security Program team, and the team is working with sites to help remedy deficiencies and bring all plans into compliance with DOE Notice 205.1 with *Unclassified Computer Security Program.* Once the review is completed, the CIO will make recommendations to appropriate management levels. CSPPs describe DOE organizations’ cyber security posture in areas such as threat, incident response, authentication and intrusion detection, as well as how the organization has chosen to comply with various security directives. For more information, contact Mike Robertson, Cyber Security team lead for CSPPs, (Telephone: 301-903-4706 or email: michael.robertson@hq.doe.gov).

CITIS: Security in Depth

The Common Information Technology Infrastructure Services (CITIS) Pilot Program is in the early stages of security project definition and will evolve in response to work on the Cyber Security Architecture. IT Infrastructure Security will support “Security in Depth,” an approach that includes technical mechanisms and operational practices to construct a consistent security infrastructure.

Technical mechanisms will include the use of firewalls, access control lists, virus scanning, filtering routers, and intrusion detection. Operational practices will include security audits, monitoring, and administration. Security in Depth will employ an array of enabling products to secure various levels of DOE’s networks. Products will protect networks from IP spoofing and eavesdropping. They will protect host-level operating systems from unauthorized access and reconfiguration. The corporate application level will require access based on user identity and role and will employ other security features embedded in the software.

National Plan Secures Cyberspace

In May 1998, Presidential Decision Directive 63 called for development of a plan to defend national cyberspace. The National Plan for Information Systems Protection Version 1.0, issued this year, is the first step in designing a method for critical infrastructure protection. It calls for the Federal government to become a model of computer system security, and it builds a cyberspace defense that relies on new security standards, multi-layered defensive technologies, new research, and trained people. The Plan aims to achieve an initial operating capability by December 2000, and a full operating capability by May 2003.

If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack.
--William J. Clinton,
President of the United States

For more information about the National Plan for Information Systems Protection and Presidential Decision Directive 63, visit the Critical Infrastructure Assurance Office’s web site (http://www.ciao.gov/National_Plan/national_plan%20_final.pdf) and (http://www.ciao.gov/press_release/WhiteHouseFactSheet_PDD63.htm).

Cyberalarm Net Considered

The Federal CIO Council is working with a bevy of security groups to form plans for a network to quickly alert Federal IT personnel to virus warnings and cyber attacks. When the “love bug” virus hit on May 4, many agencies were affected and had taken down their e-mail systems hours before alerts were issued by the Federal Computer Incident Response Capability (FedCIRC) and the National Infrastructure Protection Center (NIPC). FedCIRC resorted to faxing alerts to agencies, but with no guarantee that the messages ever reached the correct IT personnel.

The Federal CIO Council’s Security Committee, co-chaired by DOE CIO John Gilligan, is recommending that, via an intranet or wireless system, the CIO Security Network could disseminate information about viruses or cyber attacks to each agency as soon as attacks are identified. The network would give CIOs and top information security professionals the ability to securely share information about cyber attacks and download solutions or patches.